

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for securely controlling transmission of digital data comprising the steps of:
 - receiving said digital data;
 - grouping said digital data into a number of data segments by a computer;
 - forming a first segment checksum for each said data segment in accordance with a ~~method for forming type selected from the group consisting of a hashing value and a cryptographic one-way function;~~
 - forming a first commutative checksum by a commutative operation on said first segment checksums, wherein flow control for the data segments is negated by the commutative operation; and
 - cryptographically protecting said first commutative checksum by using a cryptographic operation.
2. (Currently Amended) A method for securely controlling transmission of digital data comprising the steps of:
 - receiving said digital data;
 - grouping the digital data into a number of data segments by a computer;
 - allocating a predetermined cryptographic commutative checksum to said digital data;
 - subjecting said cryptographic commutative checksum to an inverse cryptographic operation to form a first commutative checksum;
 - forming a second segment checksum for each said data segment in accordance with a ~~type selected from the group consisting of a hashing value and a cryptographic one-way function;~~

forming a second commutative checksum by a commutative operation on said second segment checksums wherein flow control for the data segments is negated by the commutative operation; and

checking said second commutative checksum for a match with said first commutative checksum.

3. (Previously Presented) A method for forming and checking a first commutative checksum for digital data comprising the steps of:

grouping said digital data into a number of data segments by a computer;

forming a first segment checksum for each said data segment in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function;

forming said first commutative checksum by a commutative operation on said first segment checksums, wherein flow control for the data segments is negated by the commutative operation;

cryptographically protecting said first commutative checksum by using at least one cryptographic operation, which forms a cryptographic commutative checksum;

subjecting said cryptographic commutative checksum to an inverse cryptographic operation to form a reconstructed first commutative checksum;

forming a second segment checksum for each said data segment of said digital data to which said first commutative checksum is allocated;

forming a second commutative checksum by a commutative operation on said second segment checksums wherein flow control for the data segments is negated by the commutative operation; and

checking said second commutative checksum for a match with said reconstructed first commutative checksum.

4-9 (Canceled).

10. (Currently Amended) ~~An apparatus~~ An arrangement for forming a first commutative checksum for digital data which are grouped into a number of data segments; said arrangement comprising:

an arithmetic and logic unit[[:]] configured to:

~~form~~ a first segment checksum, ~~which is formed~~ for each [[said]] of a plurality of data segment ~~segments~~ in accordance with a ~~method of forming type selected from the group consisting of~~ a hashing value; and a cryptographic one-way function;

~~perform~~ a commutative operation which forms [[said]] a first commutative checksum by operating on said segment checksums wherein flow control for the data segments is negated by the commutative operation[[:]]; and

~~perform~~ a cryptographic operation which cryptographically protects said first commutative checksum.

11. (Currently Amended) An ~~apparatus~~ arrangement for checking a predetermined first commutative checksum which is allocated to digital data which are grouped into a number of data segments; said arrangement comprising:

an arithmetic and logic unit[[:]] configured to:

~~form~~ a first segment checksum; ~~formed~~ in accordance with a ~~type selected from the group consisting of~~ a hashing value and a cryptographic one-way function;

~~perform~~ an inverse cryptographic operation to form a first cryptographic checksum from a cryptographic commutative checksum formed by a cryptographic operation wherein flow control for [[the]] data segments is negated by the commutative operation;

~~form~~ a second segment checksum ~~which is formed~~ for each [[said]] data segment, wherein said second segment checksum is formed in accordance with a ~~type selected from the group consisting of~~ a hashing value and a cryptographic one-way function; and

~~perform~~ a commutative operation which operates on said second segment checksums which forms a second commutative checksum wherein flow control for the data segments is negated by the commutative operation; and

a comparator ~~which checks~~ configured to check for a match between said second commutative checksum and said first commutative checksum.

12. (Currently Amended) An apparatus arrangement for forming and checking a first commutative checksum for digital data which is grouped into a number of data segments, said apparatus arrangement comprising:

an arithmetic and logic unit configured to: [[,]]

form a first segment checksum, ~~which is formed~~ for each said data segment in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function,

perform a commutative operation which forms said first commutative checksum by operating on said first segment checksums wherein flow control for the data segments is negated by the commutative operation,

perform a cryptographic operation which cryptographically protects said first commutative checksum,

form a cryptographic commutative checksum ~~formed~~ by said cryptographic operation,

perform an inverse cryptographic operation to form a first commutative checksum from said cryptographic commutative checksum,

form a second segment checksum ~~which is formed~~ for each said data segment of said digital data to which said first commutative checksum is allocated,

perform a commutative operation which operates on said second segment checksums which forms a second commutative checksum wherein flow control for the data segments is negated by the commutative operation, and

a comparator ~~which checks~~ configured to check for a match between said second commutative checksum and a reconstructed first commutative checksum, wherein said first and second segment checksum are formed in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function.

13-21. (Canceled).

22. (Previously Presented) A method according to claim 1, wherein:
said cryptographic operation is an operation selected from the group consisting of
a symmetric cryptographic method and an asymmetric cryptographic method.

23. (Previously Presented) A method according to claim 2, wherein:
said cryptographic operation is an operation selected from the group consisting of
a symmetric cryptographic method and an asymmetric cryptographic method.

24. (Previously Presented) A method according to claim 3, wherein:
said cryptographic operation is an operation selected from the group consisting of
a symmetric cryptographic method and an asymmetric cryptographic method.

25. (Previously Presented) A method according to claim 1, wherein:
said commutative operation exhibits the property of associativity.

26. (Previously Presented) A method according to claim 2, wherein:
said commutative operation exhibits the property of associativity.

27. (Previously Presented) A method according to claim 3, wherein:
said commutative operation exhibits the property of associativity.

28. (Previously Presented) A method according to claim 1, wherein said digital data
and the first cryptographic, commutative checksum are archived.

29. (Previously Presented) A method according to claim 2, wherein said digital data
and the prescribed cryptographic commutative checksum have been archived.

30. (Previously Presented) A method according to claim 3, wherein said digital data
are secured which are processed corresponding to a network management protocol.

31. (Previously Presented) A method according to claim 1, further comprising the steps of:

protecting said digital data; and
processing said digital data in accordance with a network management protocol.

32. (Previously Presented) A method according to claim 2, further comprising the steps of:

protecting said digital data; and
processing said digital data in accordance with a network management protocol.

33. (Previously Presented) A method according to claim 3, further comprising the steps of:

protecting said digital data; and
processing said digital data in accordance with a network management protocol.

34-36. (Canceled)

37. (Currently Amended) An apparatus arrangement according to claim 10, wherein:
said cryptographic operation is an operation selected from the group consisting of
a symmetric cryptographic method and an asymmetric cryptographic method.

38. (Currently Amended) An apparatus arrangement according to claim 11, wherein:
said cryptographic operation is an operation selected from the group consisting of
a symmetric cryptographic method and an asymmetric cryptographic method.

39. (Currently Amended) An apparatus arrangement according to claim 12, wherein:
said cryptographic operation is an operation selected from the group consisting of
a symmetric cryptographic method and an asymmetric cryptographic method.

40. (Currently Amended) An apparatus arrangement according to claim 10 wherein said commutative operation exhibits the property of associativity via the arrangement of said arithmetic and logic unit.

41. (Currently Amended) An apparatus arrangement according to claim 11 wherein said commutative operation exhibits the property of associativity via the arrangement of said arithmetic and logic unit.

42. (Currently Amended) An apparatus arrangement according to claim 12, wherein said commutative operation exhibits the property of associativity via the arrangement of said arithmetic and logic unit.

43. (Currently Amended) An apparatus arrangement according to claim 10, wherein: said digital data and the first cryptographic, commutative checksum are archived.

44. (Currently Amended) An apparatus arrangement according to claim 11, wherein: said digital data and the prescribed cryptographic commutative checksum have been archived.

45. (Currently Amended) An apparatus arrangement according to claim 12, wherein: said digital data and the first cryptographic, commutative checksum are archived.

46. (Currently Amended) An apparatus arrangement according to claim 10, wherein: said digital data are protected via an arrangement of said arithmetic and logic unit; and said digital data are processed in accordance with a network management protocol.

47. (Currently Amended) An apparatus arrangement according to claim 11, wherein: said digital data are protected via an arrangement of said arithmetic and logic unit;
and
said digital data are processed in accordance with a network management protocol.

48. (Currently Amended) An apparatus ~~arrangement~~ according to claim 12, wherein:
said digital data are protected via an arrangement of said arithmetic and logic unit;
and
said digital data are processed in accordance with a network management
protocol.